

**MARITIME CYBER SECURITY: A COMPARATIVE ANALYSIS OF U.S.
AND INTERNATIONAL REGULATION ON AIS DATA RECEPTORS**

An Undergraduate Research Scholars Thesis

by

SARAH ANNE HAMROCK

Submitted to the Undergraduate Research Scholars program at
Texas A&M University
in partial fulfillment of the requirements for the designation as an

UNDERGRADUATE RESEARCH SCHOLAR

Approved by Research Advisor:

Dr. Joan Mileski
Dr. Cassia Bomer Galvao

May 2019

Major: Maritime Administration

TABLE OF CONTENTS

	Page
ABSTRACT	1
DEDICATION	3
ACKNOWLEDGMENTS	4
NOMENCLATURE	5
CHAPTERS	
I. INTRODUCTION	6
II. LITERATURE REVIEW	8
Thesis Statement.....	11
Theoretical Framework	12
Project Description	13
III. WHAT IS AIS AND HOW IT WORKS IN MARITIME SHIPPING	14
3.1 International Laws: International Maritime Organization.....	15
3.2 National Laws: United States	20
IV. DATA ANALYSIS	29
4.1 Methodology.....	29
4.2 Comparative Analysis	29
V. CONCLUSION	41
REFERENCES	42

ABSTRACT

Maritime Cyber Security: A Comparative Analysis Of U.S. And International Regulation On AIS Data Receptors

Sarah Hamrock
Department of Maritime Administration
Texas A&M University

Research Advisor: Dr. Joan Mileski
Department of Maritime Administration
Texas A&M University

Cyber security is a problem within the maritime industry because of the introduction and continuous implementation of technologies, including automation and digitization of processes among others. This consequently adds new vulnerabilities within ports, ships, offshore rigs and submersibles systems. As a result, recent number of incidents show that commercial shipping has taken a more reactive than proactive approach. Compared to other industries, the maritime sector does not employ centralized monitoring of information flow through traffic controllers, like aviation. This means that any device using Internet of Things (IoT) can transmit and receive information that is captured and shared for various (unknown) purposes. This is the case with Automatic Identification System (AIS) data that has proliferated. and has potentially become a target for cyber-attack. Is every ship equipped with AIS devices? Are there rules for sending and receiving the AIS data? What is/are the enforcement mechanisms? Why should commercial maritime companies care? In this sense, this research examines the regulation on AIS data transmitters and receptors. The analysis is conducted with a comparison of international and national laws. The International reference is the IMO (International Maritime Organization) and as National (the United States), as one of the top countries targeted for cyber-attacks. The results

show that international regulation is broad and United States regulation is more restrict and specific.

DEDICATION

I dedicate this research to my parents, Gregory and Leona Hamrock, my sister, Rachel Hamrock, and my grandparents, Emma Lee and Alfred “Al/Fred” Hamrock, as well as my God who gave me the opportunity and find a passion and my purpose into helping others, specifically within the maritime industry. I also want to dedicate to my mentors and advisors, Dr. Joan Mileski, Dr. Cassia Galvao, and John Hark because you help me grow as a person not only professionally but also personally while also helping me stay on the right track and keep my foot on the gas. Thank you.

ACKNOWLEDGEMENTS

I would like to thank my advisors Dr. Joan Mileski and Dr. Cassia Galvao for encouraging me and guiding me through this exciting opportunity to gain knowledge through research.

I would also give special thanks to my friends and colleagues at the Department of Maritime Administration as well as the staff for making my time at Texas A&M University at Galveston a memorable experience. I also appreciate everyone else involved in helping me progress my research that I have such a desire to learn more about.

Conclusively, a particular thank you for my parents as they were very supportive and my sister who keeps encouraging me to be my absolute best.

NOMENCLATURE

AIS	Automatic Identification System
CFR	Code of Federal Regulations
GT	Gross Tonnage
IMO	International Maritime Organization
IoT	Internet of Things
SOLAS	Safety of Life at Sea
USCG	United States Coast Guard
VHF	Very High Frequency

CHAPTER I

INTRODUCTION

Cyber security in commercial maritime shipping is easily recognized as a sub-set of activities within the maritime business sector. The project considers three fronts in relation to cyber risk assessment: the operational characteristics; the level and detail of information; and the end-user relationship with cyber technologies. In this sense, within this research, we are using the risk assessment methodology provided by U.S. Coast Guard (USCG) to map the threats, vulnerabilities and consequences of the proliferation of AIS data in commercial maritime shipping. Consequences, otherwise known as assets, refer to the value for the company; for example, within the maritime industry, a ship would be a prime example. It is then important to identify the vulnerabilities on the ship as a shipping company can reduce its vulnerabilities easier. Threats are difficult to map due to the stigma of “we don’t know what we don’t know.”

Providing a focus on the commercial sector of shipping, specifically towards the user-perspective as well as management-based, within this project will display a cost-centered approach to making decisions within corporations. As a result, the understanding of this approach will show how much the company’s risks will cost and increases the chances of being able to purchase an insurance policy. The insurance policy’s intended goal is to reduce the risk on the number of incidences detected.

This thesis utilizes risk assessment while examining laws pertaining to AIS data in the Gulf of Mexico while also analyzing these laws currently enforced regarding AIS data as well as applied to the United States. This thesis contains two chapters.

Chapter I presents specific information regarding AIS data, its specifics within a ship, and so forth. The current laws, or lack thereof, represent the seriousness of this problem that will

harm companies in commercial maritime shipping. Included are rules from IMO (e.g. SOLAS) and USCG CFR (first sourced from the USCG's Navigation Center).

Chapter II evaluates the AIS laws in a comparative analysis focusing on transmitters and receptors. Additionally, this chapter maps out the AIS receptors/receivers, initiating that these systems are considered vulnerable for maritime companies as well as for the cyber infrastructure within the maritime industry.

CHAPTER II

LITERATURE REVIEW

Using the word “cyber” is a shortened expression for cyberspace. As stated by Biener et al (2014), cyber space is recognized to represent the interactive domain that comprises all digital networks used to store, modify and communicate information. This definition comprises all information systems that businesses, infrastructure and services depend on for support techniques. Cyber risk is relevant to cyberspace due to the basis of how both insurance and financial markets are regulated to, say, operational risks; a company must identify its vulnerabilities as well as map out threats in order to understand the risk within.

Cyber risk, included in Biener et al (2014), is referenced to a variety of risks that affect the firm’s assets informationally and technologically. One form similar to this that both affects the average person as well as a multi-billion-dollar shipping firm includes identity threat. Cyber risk also is referred to the involvement with malicious electronic events that cause the disruption of business and monetary loss (Mukhopadhyay et al (2005)). In addition, there are risks involved in a failing information system; with this considered, cyber risk is also referred to as information security risk. In Ferber (2013), many diverse economies globally are latching onto the IoT within business models that are specifically more web-based than the former.

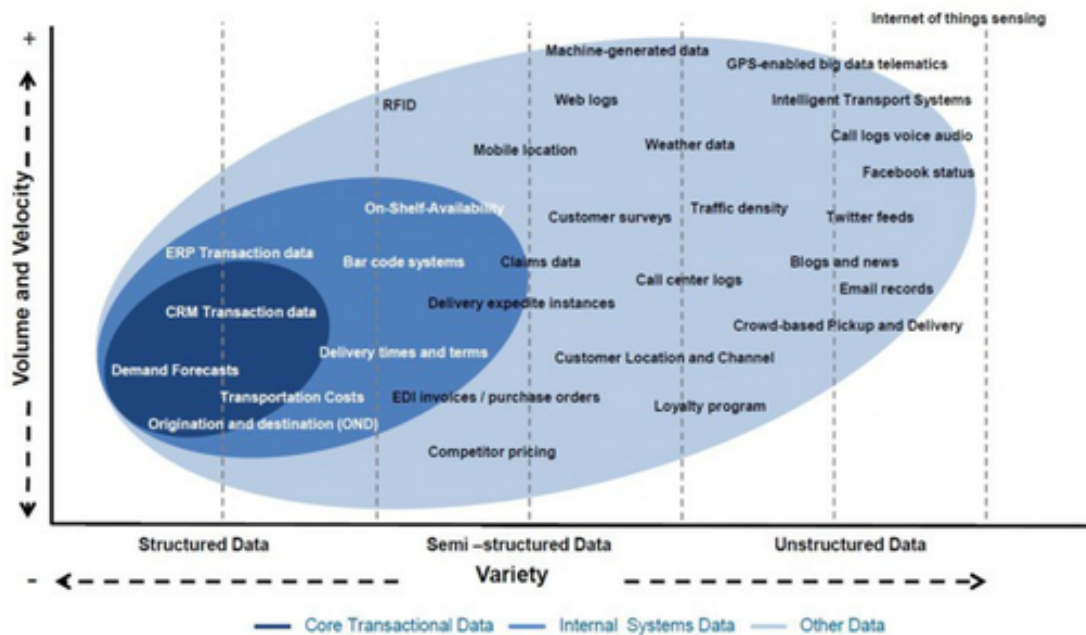
Cyber security within the maritime industry is a re-introduced notion due to new innovations modifying not only terminology used in the industry but also the way business is operated within the industry. In this part, various terms and concepts are displayed that affect the maritime sector, yet there is not a universal term to define its potency. Focusing primarily on the commercial side, searching for terms that are useful to understand for the present and the future

of the maritime industry is worthy for investigation, as this is the direction for the way the industry is leading.

Maritime cybersecurity is a rapidly growing division within the maritime industry, due to the continuous technological innovations and advancements. As a result, there is a disconnect with the maritime sector in its means to catch-up, causing vulnerabilities as well as threats to protrude. The research by the United States Coast Guard (USCG) (2008), the International Maritime Organization (IMO) (2002), and other maritime- and non-maritime-concentrated institutions also identify that these issues need to be recognized and to have efforts in place to mitigate these from occurring once more. To determine the importance of cyber security in its relationship to technological advancements such as the Automatic Identification System (AIS), it is vital to identify the terms and their relationship with these technological developments.

Recent research by Wang and Mileski (2018) has demonstrated that the maritime industry is behind in regard to the application of business strategy when compared to other international business sectors. This includes cyber infrastructure of ships, ports, offshore rigs and submersibles, which are continuously introduced as result of the incorporation of technology and among other factors, the automation and digitization of processes. Considering its nature, purpose and functionalities, the maritime industry is exposed to cyber risk, which is potentially increased with the exponential use of Internet of Things (IoT). As displayed in Figure 1, utilizing IoT is efficient and fast, but it is significantly unstructured (Robinson, 2015).

Figure 1: Data Analytics In Terms of Volume and Velocity vs. Variety



Source: Robinson (2015)

This constitutes a revolutionary force in the maritime industry due to an increase in the velocity (speed), variety, and volume of information being available. However, as a result, new vulnerabilities to the maritime industry were added and recent incidents show the sector has taken a more reactive than proactive approach. Kusi (2015) has identified threats and vulnerabilities of certain ports, giving brief insight of other issues that can promote cyber security threats and vulnerabilities. In fact, cyber risk is part of risk assessment that any organization (commercial, military, etc.) should have and, as such, several aspects could be taken in consideration depending on the threats and consequences mapped. Fitton (2015) shows the effects of extensive security of cyber aspects, such as defense and offense and the pattern of investment, will change within the future. Any risk assessment should consider at least three levels of analysis, including the physical, the legal and economical. Salem (2018) addresses that the prime action to find cyber threats and vulnerabilities is to “conduct cybersecurity risk

assessments.” The problem of cyber risk is precisely its potential devastating consequences in all of these three levels and beyond (like financial reputation and environmental damages). Lacy et al. (2014) addresses this issue, mentioning that few companies successfully generated new revenue and efficient business models. Differently from other industries, like Aviation, in maritime there is no centralized overview over the information flow through traffic controllers. In other words, this means that any device on a ship using IoT can transmit and receive information that is captured, stores, and shared to various (unknown) purposes (Robinson, 2015). This is the case with Automatic Identification System (AIS) data has proliferated and is being commercialized by various, but data accuracy is yet to be improved (Mileski et al, 2018).

This literature indicated that while relevant and widely used by maritime shipping companies, AIS data transmission and reception represent a threat in the realm of maritime cyber security. The literature on transmitters and receivers is concentrated in technical aspects and as such, we identify a gap in the analysis in the regulation of AIS data devices as such, this is the focus of this research.

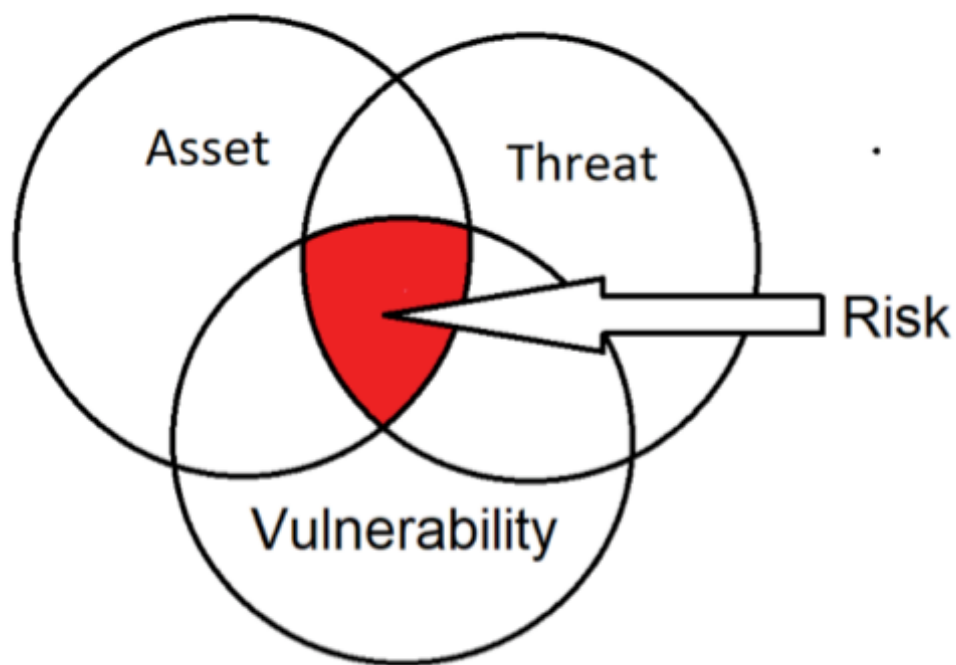
Thesis Statement

The AIS as technology is not new in its applications to commercial maritime shipping, but because of IoT, the AIS data proliferation represents a threat to the maritime cyber security. While the current literature focus on technical aspects, we state there is a need of comparing the sufficiency and enforcement of existing laws associated with AIS transmission and reception. Being United States one of the most targeted countries for cyber-attacks, we examine the U.S. laws in a comparative analysis with international regulation determined by the IMO.

Theoretical Framework

This research employs the framework provided USCG for risk assessment. According to this framework, risk can be assessed as mapping of the threats vulnerabilities and consequences. Figure 2 illustrates that overlap, being assets the corresponding variable for consequences.

Figure 2: The Cyber Risk Assessment



Sourced by: Hsia (2017)

Hsia (2017) parallels with the later-discussed United States Coast Guard (USCG) risk assessment; however, further explaining that not only should a company identify its threats and vulnerabilities, but also to assess the company's assets that have the highest impact along with value and risk, portrayed in Figure 2. Introducing the usage of the framework NIST (2018) provided is geared toward mitigating and reducing such cybersecurity risks. Fitton et al (2015)

has shown how the effects of extensive security of cyber aspects, such as defense and offense and the pattern of investment, will change within the future. Any risk assessment should consider at least three levels of analysis, including the physical, the legal and economical. Salem (2018) addresses that the prime action to find cyber threats and vulnerabilities is to “conduct cybersecurity risk assessments.” The problem of cyber risk is precisely its potential devastating consequences in all of these three levels and beyond like financial reputation and environmental damages. In our case, the proliferation of AIS data is considered the threat and the regulation a vulnerability on the national security level in commercial maritime shipping. Additional research would be required to map other vulnerabilities on commercial companies’ level as well as the consequences.

Project Description

This research can be described as comparative analysis of AIS regulation in the international and national jurisdiction. The comparison uses secondary data provided by International Maritime Organization (IMO)/Safety of Life at Sea (SOLAS) and United States Coast Guard (USCG)/Code of Federal Regulations (CFR). I use the IMO for investigating the existence of sufficiency and enforcement of regulation pertaining to AIS transmitters and receptors for commercial maritime shipping (military use is excluded here). United States was selected as the national case to be studied considering the relevance of maritime industry to the country economy (include here the 90% of everything) and the fact that is one of the top 10 countries targeted for cyber attacks. The analysis leads us to the following results, such as insufficiency due to laws lacking in depth enforcement and laws that do not cover all risks. These two categories identifying can lead to loopholes within these laws.

CHAPTER III

WHAT IS AIS AND HOW IT WORKS IN MARITIME SHIPPING

AIS is defined as the Automatic Identification System. Title 33, Code of Federal Regulations § 164.46 Automatic Identification System (2015) expresses that AIS is the communication system that ships refer back to for safety and navigational purposes. AIS includes data relative to the vessel, such as what the vessel looks like, where the vessel is located, the speed of the vessel, and other relevant safety information whether that is from an exchange of data and communication from ship to ship or ship via server. In addition, the vessel can also receive data such as port information.

There are currently three types of AIS equipment: Class A, Class B, and receive only. Class A is required for vessels over 300GT (ongoing international voyages) and vessels over 150GT but is allowed for vessels less than 150GT that would normally be eligible for Class B AIS equipment (FOOTNOTE: SOLAS 2.2). Class A AIS equipment transmits more information and a higher speed and power than Class B while also receiving data at a quicker pace. Both Class A and B, however, are required to obtain a GPS receptor due the ability to manage vessels' precise timing, derived from GPS (per RayMarine). The receiving only category includes utilizing AIS data from the Internet by AIS providers. The business these providers make is to sell the data by collecting the data from numerous receiving points and amassing these data into the big picture. Vulnerabilities occur within this market, however. There are gaps in certain areas where signals will not pick up. Additionally, false reporting, spoofing, and multipathing and ghost-targeting remain difficult to prevent and reduce within this specific area. Furthermore, a professional at RayMarine mentioned that these data providers are not transmitting via VHF; instead, these providers are transmitting data to the Internet via phone data system.

Access to receive AIS information throughout the global via satellite is a recent advancement. There are numerous AIS data providers that grant the user access normally through a subscription, usually aimed to aid fleet operators. Most commonly used include MarineTraffic (a Greek data provider), exactEarth (a Canadian data provider) and many more. Additionally, AIS receiver equipment may include two receivers for monitoring frequency purposes.

3.1 International Laws: IMO

The Automatic Identification System (AIS) that is properly installed will need to comply with the guidelines of the International Maritime Organization (IMO) Resolution A.917(22) as well as the Safety of Navigation Circulars (SN/Circ.) 227, 244, 245, and SN.1/Circ.289; or National Marine Electronics Association (NMEA) Installation Standard 0400-3.10 in lieu of SN/Circ. 227 and 245 (reference § 164.03). The International Telecommunication Union is in charge of not only recognizing the characteristics within AIS but also in the relationship with VHF mobility, which resulted in the action of the International Maritime Organization (IMO) to adopt these as a prototype for standards in AIS technology. Additionally, the International Association of Marine Aids to Navigation and Lighthouse Authorities (IALA) (2016) presents many laws that, while in cooperation with IMO (recognizing its involvement with the IMO), are to be followed in regard to AIS data (Table 1). The following includes a list of international laws in relation to AIS data from the IALA.

Table 1: Contains laws established within the IALA.

LAW	DESCRIPTION
3.1.1. TIMING	Ensure that the devices are synchronized (2250 slots per minute), every AIS needs to contain the following system: Global Navigation Satellite Receiver System (GNSS, for example, the Global Positioning system GPS), providing the universal time coordinated (UTC) as a reference. If this becomes lost, synchronization is provided by other mobile units or AIS Base Stations in the area.
3.2 VHF DATA LINK	The AIS has been designed for short range, VHF coverage, normally referred to as ‘line of sight’. Although most AIS messages only use one (1) slot, some can occupy up to five (5) consecutive time slots. The greater the number of slots used by a message, and the larger the number of vessels in a coverage area, the greater the potential for the data packet (slot) collisions. Since most AIS base stations typically have a high antenna position, large coverage area, this may result in messages not being, large coverage area, this may result in messages not being decoded from more distant AIS units in an area where there are a very large number of AIS stations operating. However, data from these distant stations would continue to be transmitted and received correctly by closer AIS stations. Class A stations also broadcast a Long Range AIS broadcast Message (Message 27) every 3 minutes on two VHF channels 75 (AIS3) and 76 (AIS4) for satellite reception. This message should be suppressed when the Class A station is within an AIS Base station coverage area by the group assignment message from the controlling base station.
3.4. DISPLAY OF AIS DATA	AIS data can be displayed in different ways. AIS class A must have a Minimum Keyboard and Display (MKD), primarily intended for installation but displaying AIS target, name, bearing and range. On vessels with AIS compliant navigational displays (IEC 62288), the manner in which targets are displayed depends on the type of AIS data: Ship dynamic data are typically displayed as triangular shaped icons (see Figure 2); Ship static data is typically shown as a textbox; Safety messages are also shown as a textbox; AIS AtoN messages as diamond shaped icons. Meteorological and hydrological data in alphanumeric and / or in a graphical manner.

3.6.3.6. CHANNEL MANAGEMENT	Channel management provides the ability to ‘require’ ships within a defined area to transmit and receive AIS on frequencies other than the two international dedicated AIS frequencies (AIS1, AIS2). This can be accomplished by sending a channel management message on the existing AIS frequencies or on DSC (Digital Selective Calling) channel 70. The alternate channel(s) chosen must be free from other VHF traffic. This channel management can be used where the existing AIS frequencies are not available for use, if there is interference on existing AIS frequencies or in areas of high activity on the VDL (VHF Data Link).
-----------------------------------	--

Source: Author own elaboration based on IALA AIS Guidelines (2016)

According to SOLAS Annex 17 – Automatic Identification System (AIS) (2002) (featured in Table 2), shipborne AIS systems nonstop transmits data to each other via vessel to vessels and VTS stations. Suitable graphical display needs to be utilized as AIS sourced on vessel is facilitates quick performance of involuntary information, using Closest Point of Approach (CPA) and Time to Closest Point of Approach (TCPA) from the position information transmitted by the target vessels.

Table 2: Contains the laws and regulations for AIS receivers/receptors in IMO SOLAS Annex 12 & Annex 17

LAW	DESCRIPTION
IMO: Annex 12.1(a)	Adopts recommendation on Performance Standards for Shipborne Combined GPS/GLONASS Receiver Equipment
IMO: Annex 12.1.1.2.	A combined receiver, when compared to either the GPS or GLONASS receiver, offers improved availability, integrity, accuracy and resistance to interference; increased ease of installation, and the ability to operate in the differential GPS mode (DGPS), differential GLONASS (DGLONASS) mode and the combined DGPS and DGLONASS mode, when available.
IMO: Annex 12. 3.1.1.1	Performance Standards for Combined GPS/GLONASS Receiver Equipment; The combined GPS/GLONASS receiver equipment should: be capable of receiving and processing Standard Positioning Service (SPS) signals of the GPS as modified by Selective Availability (SA)

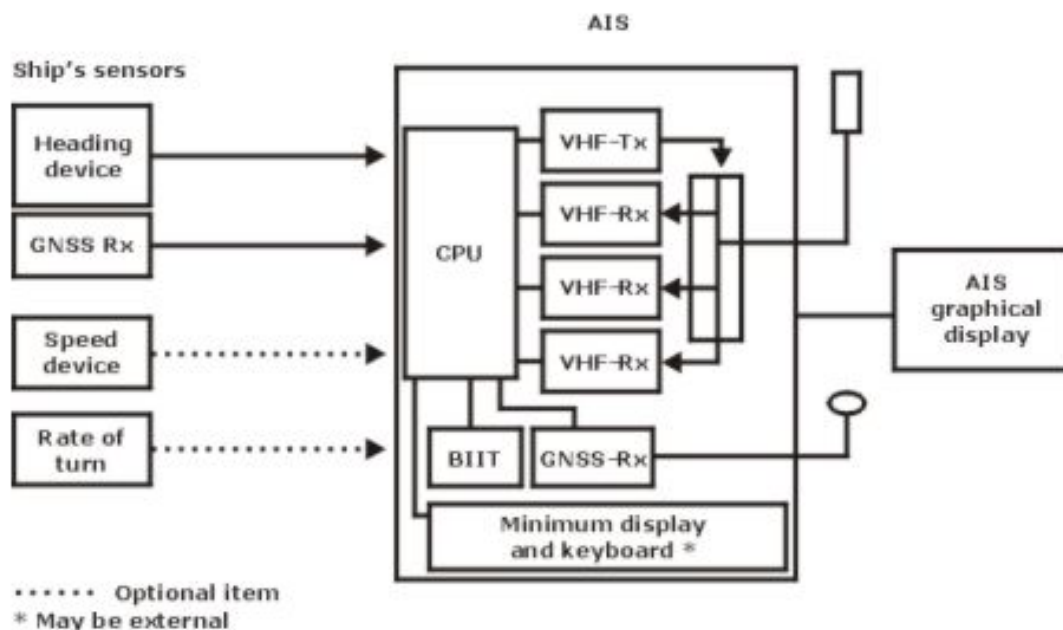
	and range code signals in GLONASS and provide position information in latitude and longitude World Geodetic System (WGS) 84 co-ordinates in degrees, minutes and thousandths of minutes... Where the facility exists, the display and any data output should indicate that the co-ordinate conversion is being performed and should identify the co-ordinate system in which the position is expressed;
12.3.3.1.3	The AIS should comprise a means to automatically input data from other sensors meeting the provisions as specified in paragraph 6.2
12.3.3.1.4	CAPABILITY The AIS should comprise: a means to input and retrieve data manually.
12.3.3.1.5	The AIS should comprise a means of checking the transmitted and received data
IMO: Annex 12.3.2.1	The AIS should be capable of: providing information automatically and continuously to a competent authority and other ships, without involvement of ship's personnel;
IMO: Annex 12.3.2.2	The AIS should be capable of: receiving and processing information from other sources, including that from a competent authority and from other ships;
IMO: Annex 12.3.2.3	The AIS should be capable of: responding to high priority and safety related calls with a minimum of delay; and
IMO: Annex 12.3.2.4	The AIS should be capable of: providing positional and maneuvering information at a data rate adequate to facilitate accurate tracking by a competent authority and other ships.
IMO: Annex 17.35	INHERENT LIMITATIONS ON AIS: The accuracy of AIS information received is only as good as the accuracy of the AIS information transmitted.
IMO: Annex 17.38	INHERENT LIMITATIONS ON AIS: It would not be prudent for the OOW to assume that the information received from other ships is of a comparable quality and accuracy as that which might be available on own ship.
Annex 17.44	AIS IN VTS OPERATIONS: Pseudo AIS Information: VTS centres may send information about vessels which are not carrying AIS and which are tracked only by VTS radar, via the AIS to vessels equipped with AIS. Any pseudo AIS target broadcast by VTS should be clearly identified as such. Particular care should always be taken when using information which has been relayed by a third party. Accuracy of these targets may not be as accurate as actual directly-received targets and the information content may not be as complete.

Source: Author own elaboration based on IMO SOLAS Annex 12 and 17 (2002)

To note, Annex 17.51.1 also consists of the following equipment: antennas, one VHF transmitter; two multi-channel VHF receivers; one channel 70 VHF receiver for channel

management; a central processing unit (CPU); an electronic position fixing system, Global Navigation Satellite System (GNSS) receiver for timing purpose and position redundancy; interfaces to heading and speed devices and to other shipborne sensors; interfaces to heading and speed devices and to other shipborne sensors; interfaces to radar/Automatic Radar Plotting Aids (ARPA), Electronic Chart System/Electronic Chart Display and Information System (ECS/ECDIS) and Integrated Navigation Systems (INS); BIIT (Built In Integrity Test); and minimum display and keyboard to input and retrieve data. Figure 3 will allow visualization on these systems and allow a basis for understanding these systems.

Figure 3: The Components of an onboard AIS



Sourced by: SOLAS (2015) Annex 17 51.1

Figure 3 depicts the general requirements of the AIS receptors/receivers in that it only specifically states that the receiver retrieves data that is sent to the Central Processing Unit (CPU) within the system. Due to the goal of increasing its effectiveness, allowing AIS to operate

similar to a stand alone system, it would have to include a graphical display or the integration of the AIS data display in devices such as INS (Integrated Navigation System), ECS/ECDIS (Electronic Chart System/Electronic Chart Display and Information), or radar displays. Additional information includes that the AIS can either connect to an additional dedicated AIS display unit or to an existing navigational system such as ECS/ECDIS, radar, and/or participate with integrating with an existing navigation system (SOLAS Annex 17, 51.5).

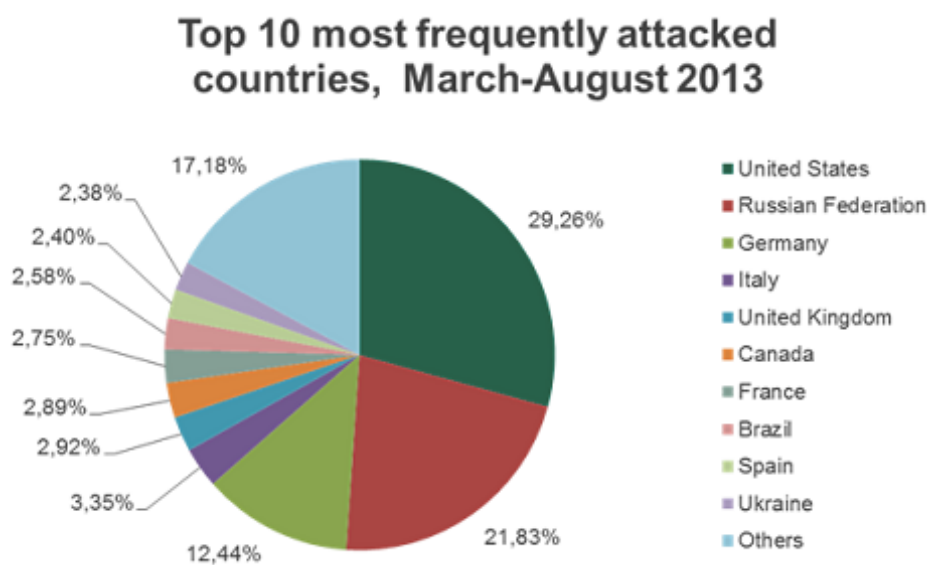
On board AIS data information is both transmitted uninterruptedly and automatically without any intervention or knowledge of the officer of the watch (OOW). Fitting to Annex 17 (2002), an AIS station might require updates on information from a specific ship by “polling” that ship, or alternatively, might wish to “poll” all ships within a defined sea area. However, the shore station can only increase the ships’ reporting rate but not decrease it. The AIS information transmitted by a ship is of three different types: fixed (also known as static) information, which is entered into the AIS through installation and need only be changed if the ship changes its name or undergoes a major conversion from one ship type to another; dynamic information, which, apart from ‘Navigational status’ information, (automatically updates from the ship sensors connected to AIS); and voyage-related information, (manual input and updated during the voyage).

3.2 National Laws: United States

The United States Coast Guard initiated rules regarding the AIS onboard ships. Here, the CFR displays the IMO SOLAS Annex 12 and 17 laws on a significantly descriptive level. This is shown in Figure 4, where the US shares slightly more than a quarter of the pie chart. As a main target for attacks, namely in maritime, laws need to cause awareness to these vulnerabilities. In addition, laws may continue in gaps, or loopholes, that make it simpler for hackers and terrorists

to infiltrate systems, such as AIS data, remotely. The United States Coast Guard established the Code of Federal Regulations (CFR) in ways that vessels and maritime entities can comply and mitigate issues and attacks due to vulnerabilities. Violation of these laws includes penalties such as fines for each violation committed in that period (43-46 CFR), further explained at the near-end of the paper. Due to the strength, or lack thereof, may cause a loophole in the laws that should be addressed.

Figure 4: The top-Ten Frequently Cyber-Attacked Countries



Source: Kaspersky Lab (2013)

Table 3: Contains the laws and regulations for AIS and AIS receivers/receptors under the United States Coast Guard Code of Federal Regulations (CFR).

LAW Title 33, Code of Federal Regulations (AIS REQUIREMENTS)	DESCRIPTION
<i>§ 164.01 Applicability</i>	<p>(a) This part (except as specifically limited by this section) applies to each self-propelled vessel of 1600 or more gross tons (except as provided in paragraphs (c) and (d) of this section, or for foreign vessels described in §164.02) when it is operating in the navigable waters of the United States except the St. Lawrence Seaway.</p> <p>(b) * * *</p> <p>(c) Provisions of §§ 164.11(a)(2) and (c), 164.30, 164.33, and 164.46 do not apply to warships or other vessels owned, leased, or operated by the United States Government and used only in government noncommercial service when these vessels are equipped with electronic navigation systems that have met the applicable agency regulations regarding navigation safety.</p> <p>(d) Provisions of § 164.46 apply to some self-propelled vessels of less than 1600 gross tonnage.</p>
<i>§ 164.46 Automatic Identification System</i>	<p>(a) Definitions. As used in this section— <i>Automatic Identification Systems</i> or <i>AIS</i> means a maritime navigation safety communications system standardized by the International Telecommunication Union (ITU), adopted by the International Maritime Organization (IMO), that--</p> <p>(1) Provides vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft;</p>

<p>§ 164.46 Automatic Identification System</p>	<p>(2) Receives automatically such information from similarly fitted ships, monitors and tracks ships; and</p> <p>(3) Exchanges data with shore-based facilities.</p> <p><i>Gross tonnage</i> means tonnage as defined under the International Convention on Tonnage Measurement of Ships, 1969.</p> <p><i>International voyage</i> means a voyage from a country to which the present International Convention for the Safety of Life at Sea applies to a port outside such country, or conversely.</p> <p><i>Properly installed, operational</i> means an Automatic Identification System (AIS) that is installed and operated using the guidelines set forth by the International Maritime Organization (IMO) Resolution A.917(22) and Safety of Navigation Circulars (SN/Circ.) 227, 244, 245, and SN.1/Circ.289; or National Marine Electronics Association (NMEA) Installation Standard 0400-3.10 in lieu of SN/Circ.227 and 245 (incorporated by reference, see § 164.03).</p> <p>(b) <i>AIS carriage</i>.</p> <p>(1) <i>AIS Class A device</i>. The following vessels must have on board a properly installed, operational USCG Type-approved* AIS Class A device:</p> <p>(i) A self-propelled vessel of 65 feet or more in length, engaged in commercial service.</p> <p>(ii) A towing vessel of 26 feet or more in length and more than 600 horsepower, engaged in commercial service.</p> <p>(iii) A self-propelled vessel that is certificated to carry more than 150 passengers.</p> <p>(iv) A self-propelled vessel engaged in dredging operations in or near a commercial channel or shipping fairway in a manner likely to restrict or affect navigation of other vessels.</p> <p>(v) A self-propelled vessel engaged in the movement of –</p> <p>(A) Certain dangerous cargo as defined in subpart C of part 160 of this chapter, or</p>
--	---

<p>§ 164.46 Automatic Identification System</p>	<p>(B) Flammable or combustible liquid cargo in bulk that is listed in 46 CFR 30.25–1, Table 30.25–1.</p> <p>(2) AIS Class B device. AIS Class B device in lieu of an AIS Class A device is permissible on the following vessels if they are not subject to pilotage by other than the vessel Master or crew:</p> <p>(i) fishing industry vessels;</p> <p>(ii) Vessels identified in paragraph (b)(1)(i) of this section that are certificated to carry less than 150 passengers and that–</p> <p>(A) Do not operate in a Vessel Traffic Service (VTS) or Vessel Movement Reporting System (VMRS) area defined in Table 161.12(c) of § 161.12 of this chapter, and</p> <p>(B) Do not operate at speeds in excess of 14 knots; and</p> <p>(iii) Vessels identified in paragraph (b)(1)(iv) of this section engaged in dredging operations.</p> <p>(c) <i>SOLAS provisions</i>. The following self-propelled vessels must comply with International Convention for Safety of Life at Sea (SOLAS), as amended, Chapter V, regulation 19.2.1.6 (Positioning System), 19.2.4 (AIS Class A), and 19.2.3.5 (Transmitting Heading Device) or 19.2.5.1 (Gyro Compass) as applicable (Incorporated by reference, see § 164.03):</p> <p>(1) A vessel of 300 gross tonnage or more, on an international voyage.</p> <p>(2) A vessel of 150 gross tonnage or more, when carrying more than 12 passengers on an international voyage.</p> <p>(d) <i>Operations</i>. The requirements in this paragraph are applicable to any vessel equipped with AIS.</p> <p>(1) Use of AIS does not relieve the vessel of the requirements to sound whistle signals or display lights or shapes in accordance with the International Regulations for Preventing Collisions at Sea, 1972 (72 COLREGS), 28 U.S.T. 3459, T.I.A.S. 8587, or Inland Navigation Rules, 33 CFR part 83; nor of the radio requirements of the Vessel Bridge-to-Bridge Radiotelephone Act, 33 U.S.C. 1201–</p>
--	---

<p>§ 164.46 Automatic Identification System</p>	<p>1208, part 26 of this chapter, and 47 CFR part 80.</p> <p>(2) AIS must be maintained in effective operating condition, which includes--</p> <ul style="list-style-type: none"> (i) The ability to reinitialize the AIS, which requires access to and knowledge of the AIS power source and password; (ii) The ability to access AIS information from the primary conning position of the vessel; (iii) The accurate broadcast of a properly assigned Maritime Mobile Service Identity (MMSI) number; (iv) The accurate input and upkeep of all AIS data fields and system updates; and (v) For those vessels denoted in paragraph (b) of this section, the continual operation of AIS and its associated devices (e.g., positioning system, gyro, converters, displays) at all times while the vessel is underway or at anchor, and, if moored, at least 15 minutes prior to getting underway; except when its operation would compromise the safety or security of the vessel or a security incident is imminent. The AIS should be re`ed to continuous operation as soon as the compromise has been mitigated or the security incident has passed. The time and reason for the silent period should be recorded in the ship's official log and reported to the nearest Captain of the Port or Vessel Traffic Center (VTC). <p>(3) AIS safety-related text messaging must be conducted in English and solely to exchange or communicate pertinent navigation safety information (analogous to a SECURITE broadcast). Although not prohibited, AIS text messaging should not be relied upon as the primary means for broadcasting distress (MAYDAY) or urgent (PAN PAN) communications. (47 CFR 80.1109, Distress, urgency, and safety communications).</p> <p>(4) AIS application-specific messaging (ASMs) is permissible, but is</p>
--	---

<p>§ 164.46 Automatic Identification System</p>	<p>limited to applications adopted by the International Maritime Organization (such as IMO SN.1/Circ.289) or those denoted in the International Association of Marine Aids to Navigation and Lighthouse Authorities' (IALA) ASM Collection for use in the United States or Canada, and to no more than one ASM per minute.</p> <p><i>Note to paragraph (d):</i> The Coast Guard has developed the "U.S. AIS Encoding Guide" to help ensure consistent and accurate data encoding (input) by AIS users. This Guide is available at our "AIS Frequently Asked Questions" (FAQ #2) World Wide Web page at https://www.navcen.uscg.gov. Although of great benefit, the interfacing or installation of other external devices or displays (e.g., transmitting heading device, gyro, rate of turn indicator, electronic charting systems, and radar), is not currently required except as denoted in § 164.46(c). Most application-specific messages require interfacing to an external system that is capable of their portrayal, such as equipment certified to meet Radio Technical Commission for Maritime Services (RTCM) electronic chart system (ECS) standard 10900 series.</p> <p>(e) <i>Watchkeeping.</i> AIS is primarily intended for use by the Master or person in charge of the vessel, or by the person designated by the Master or person in charge to pilot or direct the movement of the vessel, who must maintain a periodic watch for AIS information.</p> <p>(f) <i>Portable AIS.</i> The use of a portable AIS is permissible only to the extent that electromagnetic interference does not affect the proper function of existing navigation and communication equipment on board and such that only one AIS device may be transmitting on board a vessel at any one time.</p> <p>(g) <i>AIS Pilot Plug.</i> The AIS Pilot Plug on any vessel subject to pilotage by other than the vessel Master or crew must be readily available and easily accessible from the</p>
--	--

	<p>primary conning position of the vessel and permanently affixed (not an extension cord) and adjacent (within 3 feet) to a 120-volt 50/60 Hz AC power receptacle (NEMA 5-15).</p> <p>(h) <i>Exceptions.</i> The following vessels may seek up to a 5-year deviation from the AIS requirements of this section by requesting a deviation under § 164.55.</p> <p>(1) Vessels that operate solely within a very confined area (e.g., less than a 1 nautical-mile radius, shipyard, or barge fleeting facility);</p> <p>(2) Vessels that conduct only short voyages (less than 1 nautical mile) on a fixed schedule (e.g., a bank-to-bank river ferry service or a tender vessel);</p> <p>(3) Vessels that are not likely to encounter other AIS-equipped vessels;</p> <p>(4) Vessels whose design or construction makes it impracticable to operate an AIS device (e.g., those that lack electrical power, have an exposed or open cabin, or are submersible); or</p> <p>(5) Vessels denoted in paragraph (b)(2) that seek a deviation from requirements in paragraphs (d)(2)(ii) and (e) of this section because their AIS Class B device lacks a display.</p> <p>(i) <i>Prohibition.</i> Except for maritime support stations (see 47 CFR 80.5) licensed by the Federal Communications Commission (FCC), broadcasts from AIS Class A or B devices on aircraft, non-self propelled vessels or from land are prohibited.</p> <p>(j) <i>Implementation date.</i> Those vessels identified in paragraphs (b) and (c) of this section that were not previously subject to AIS carriage must install AIS no later than March 1st, 2016 [eff. 81 FR 20250, 4/7/16].</p>
<p>§ 164.46 Automatic Identification System (ADD-IN)</p>	<p><i>Note to paragraph (b):</i> Under 33 U.S.C. 1223(b)(3) and 33 CFR 160.111, a Coast Guard Captain of the Port (COTP) may restrict the operation of a vessel if he or she determines that by reason of weather,</p>

	visibility, sea conditions, port congestion, other hazardous circumstances, or the condition of such vessel, the restriction is justified in the interest of safety. In certain circumstances, if a COTP is concerned that the operation of a vessel not subject to § 164.46 would be unsafe, the COTP may determine that voluntary installation of AIS by the operator would mitigate that concern.
--	--

Source: Author own elaboration based on USCG CFR (2015)

The area of focus is on the United States laws mainly because how stringent their policies are compared with other countries around the world but also because the U.S. is the most vulnerable when it comes to cyber attacks. In a publication report by Kaspersky Lab (2013) shared that the United States is the most frequently attacked country. The US Coast Guard established the Codes of Federal Regulation (CFR) (featured in Table 3) as of March 2015 to increase the strength of the current international laws listed.

CHAPTER IV

DATA ANALYSIS

4.1 Methodology

This analysis was conducted in three steps. First, AIS regulations were collected from international and national authorities. Second, a filter in the regulation was applied to identify the specific chapters and items associated with AIS transmitters/receptors. Third, a comparative analysis was conducted using two main criteria: sufficiency and enforcement. Sufficiency is defined as *if the regulation covers description of the capability of receivers or specifies additional receiver equipment information* (Merriam-Webster 2011). In order to check on this criterium, we basically verified the existence of that information. As for enforcement, it is defined as *how the regulation is implemented and what is the process of compliance verified by the authority*. In our analysis we have verified if the regulation gives enough mechanisms of enforcement to the authority.

The data used is secondary data gathered directly from IMO/SOLAS and USCG/CFR available in their respective virtual libraries (i.e. ebscoHOST, WorldCat, GoogleScholar all which aid researchers to retrieve information at a faster pace). Being the IMO and USCG the responsible authorities in their respective international and national regulation for maritime shipping, we consider that was no need for additional step to validate their data. Finally, two tables were created to enable side-by-side comparison.

4.2 Comparative Analysis

In this section we have conducted the comparative analysis of national and international regulation on AIS data transmission and reception. These laws are distinguished by the amount

of vulnerabilities and defined if there are gaps and loopholes within these laws for receptors. Two tables (Table 4 and Table 5) are presented to identify the laws if there are gaps within enforcement and sufficiency criteria.

Table 4. INTERNATIONAL LAW: Vulnerability factors listed within the laws specifically towards AIS receivers

LAW	DESCRIPTION	SUFFICIENCY	ENFORCEMENT
IMO: Annex 12. 3.1.1	Performance Standards for Combined GPS/GLONASS Receiver Equipment; The combined GPS/GLONASS receiver equipment should: be capable of receiving and processing Standard Positioning Service (SPS) signals of the GPS as modified by Selective Availability (SA) and range code signals in GLONASS and provide position information in latitude and longitude World Geodetic System (WGS) 84 co-ordinates in degrees, minutes and thousandths of minutes... Where the facility exists, the display and any data output should indicate that the co-ordinate conversation is being performed and should identify the co-ordinate system in which the position is expressed;	SUFFICIENT: COVERS DESCRIPTION OF THE CAPABILITY OF RECEIVERS; SPECIFIES ADDITIONAL RECEIVER EQUIPMENT INFORMATION	ENFORCED: NOT NECESSARILY, DOES NOT MENTION HOW IT IS ENFORCED BUT DUE TO ITS SPECIFIC DESCRIPTION
IMO: Annex 12.3.1.4	CAPABILITY The AIS should comprise: a means to input and retrieve data manually;	SUFFICIENT: LACKING, DOES NOT SPECIFY NOR ESTABLISH THE	ENFORCED: LACKING, DUE TO DEFICIENCY IN SPECIFICATION

		MEANS, CAUSING A LOOPHOLE IN THE LAW	
IMO: Annex 12.3.1.5	The AIS should comprise a means of checking the transmitted and received data;	SUFFICIENT: LACKING, NEEDS TO SPECIFY THE MEANS	ENFORCED: LACKING, DUE TO DEFICIENCY IN SPECIFICATION
IMO: Annex 12.3.2.2	The AIS should be capable of: receiving and processing information from other sources, including that from a competent authority and from other ships;	SUFFICIENT: LACKING, DOES NOT ADDRESS AN ESTABLISHED WAY HOW (NEEDS STANDARDIZATION)	ENFORCED: LACKING, NEEDS TO SPECIFY “COMPETENT.” TOO BROAD
IMO: Annex 12.3.2.3	The AIS should be capable of: responding to high priority and safety related calls with a minimum of delay; and	SUFFICIENT: ADDRESSES SAFETY COMMUNICATION	ENFORCED: SPECIFY TYPE OF CALLS
IMO: Annex 17.35	INHERENT LIMITATIONS ON AIS: The accuracy of AIS information received is only as good as the accuracy of the AIS information transmitted.	SUFFICIENT: LACKING, NO FURTHER EXPLANATION IN REGARDS TO ACCURACY	ENFORCED: LACKING, NO FURTHER INFORMATION
IMO: Annex 17.38	INHERENT LIMITATIONS ON AIS: It would not be prudent for the OOW to assume that the information received from other ships is of a comparable quality and accuracy as that which might be available on own ship.	SUFFICIENT: ADDRESSES A REQUIRED POSITION AND ACTION	ENFORCED: NOT NECESSARILY, CONSIDERED MORE AS A SUGGESTION
IMO: Annex 17.44	AIS IN VTS OPERATIONS: Pseudo AIS Information: VTS centres may send information about vessels which are not carrying AIS and which are tracked only by VTS radar,	SUFFICIENT: COVERS DESCRIPTION OF THE CAPABILITY OF RECEIVERS; SPECIFIES	ENFORCED: DOES NOT MENTION HOW IT IS ENFORCED BUT

	via the AIS to vessels equipped with AIS. Any pseudo AIS target broadcast by VTS should be clearly identified as such. Particular care should always be taken when using information which has been relayed by a third party. Accuracy of these targets may not be as accurate as actual directly-received targets and the information content may not be as complete.	ADDITIONAL RECEIVER EQUIPMENT INFORMATION	DUE TO ITS SPECIFIC DESCRIPTION
--	--	---	---

Source: Author's own elaboration based on IMO/SOLAS (2015).

Table 5. NATIONAL (U.S.): Vulnerability factors listed within the laws specifically towards AIS receivers

LAW Title 33, Code of Federal Regulations (AIS REQUIREMENTS)	DESCRIPTION	SUFFICIENCY	ENFORCE- MENT
<i>§ 164.01</i> <i>Applicability</i>	(a) This part (except as specifically limited by this section) applies to each self-propelled vessel of 1600 or more gross tons (except as provided in paragraphs (c) and (d) of this section, or for foreign vessels described in §164.02) when it is operating in the navigable waters of the United States except the St. Lawrence Seaway. (b) * * * (c) Provisions of §§ 164.11(a)(2) and (c), 164.30, 164.33, and 164.46 do not apply to warships or other vessels owned, leased, or operated by the United States Government and used only in government	SUFFICIENT: COVERS DESCRIPTION OF THE CAPABILITY OF RECEIVERS; SPECIFIES ADDITIONAL RECEIVER EQUIPMENT INFORMATION	ENFORCED: PROVIDES ENFORCEMENT BY SPECIFYING SOLELY WHAT VESSEL IS UNDER COMPLIANCE FOR THE UNITED STATES LAW

	<p>noncommercial service when these vessels are equipped with electronic navigation systems that have met the applicable agency regulations regarding navigation safety.</p> <p>(d) Provisions of § 164.46 apply to some self-propelled vessels of less than 1600 gross tonnage.</p>		
<p>§ 164.46 Automatic Identification System</p>	<p>(a) Definitions. As used in this section--</p> <p><i>Automatic Identification Systems</i> or <i>AIS</i> means a maritime navigation safety communications system standardized by the International Telecommunication Union (ITU), adopted by the International Maritime Organization (IMO), that--</p> <p>(1) Provides vessel information, including the vessel's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships, and aircraft;</p> <p>(2) Receives automatically such information from similarly fitted ships, monitors and tracks ships; and</p> <p>(3) Exchanges data with shore-based facilities.</p> <p><i>Gross tonnage</i> means tonnage as defined under the International Convention on Tonnage Measurement of Ships, 1969.</p> <p><i>International voyage</i> means a voyage from a country to which the present International Convention for the Safety of Life at Sea applies to a port outside such country, or conversely.</p> <p><i>Properly installed, operational</i> means an Automatic Identification System (AIS) that is installed and operated using the guidelines set forth by the International Maritime Organization (IMO) Resolution A.917(22) and Safety of Navigation Circulars (SN/Circ.) 227, 244, 245, and SN.1/Circ.289; or National Marine Electronics Association (NMEA) Installation Standard 0400-3.10 in lieu of SN/Circ.227 and 245 (incorporated by</p>	<p>SUFFICIENT: ESTABLISHES SPECIFIC INFORMATION REGARDING AIS RECEPTORS, SPECIFICALLY ESTABLISHED CONDITIONS FOR THE VESSEL AND ITS SYSTEMS; EXTREMELY SPECIFIC, LENGTHY REGULATION COVERS DESCRIPTION OF THE CAPABILITY OF RECEIVERS; SPECIFIES ADDITIONAL RECEIVER EQUIPMENT INFORMATION</p>	<p>ENFORCED: PROVIDES ENFORCEMENT BY SPECIFYING SOLELY WHAT COMPLIANCE FOR THE UNITED STATES LAW AS WELL AS ITS LAW FOR INTERNATIONAL LAW; CFR IS MORE STRINGENT ON ENFORCEMENT WITH AIS LAWS</p>

<p>§ 164.46 Automatic Identification System</p>	<p>reference, see § 164.03).</p> <p>(b) <i>AIS carriage</i>.</p> <p>(1) <i>AIS Class A device</i>. The following vessels must have on board a properly installed, operational USCG Type-approved* AIS Class A device:</p> <p>(i) A self-propelled vessel of 65 feet or more in length, engaged in commercial service.</p> <p>(ii) A towing vessel of 26 feet or more in length and more than 600 horsepower, engaged in commercial service.</p> <p>(iii) A self-propelled vessel that is certificated to carry more than 150 passengers.</p> <p>(iv) A self-propelled vessel engaged in dredging operations in or near a commercial channel or shipping fairway in a manner likely to restrict or affect navigation of other vessels.</p> <p>(v) A self-propelled vessel engaged in the movement of –</p> <p>(A) Certain dangerous cargo as defined in subpart C of part 160 of this chapter, or</p> <p>(B) Flammable or combustible liquid cargo in bulk that is listed in 46 CFR 30.25–1, Table 30.25–1.</p> <p>(2) <i>AIS Class B device</i>. AIS Class B device in lieu of an AIS Class A device is permissible on the following vessels if they are not subject to pilotage by other than the vessel Master or crew:</p> <p>(i) fishing industry vessels;</p> <p>(ii) Vessels identified in paragraph (b)(1)(i) of this section that are certificated to carry less than 150 passengers and that–</p> <p>(A) Do not operate in a Vessel Traffic Service (VTS) or Vessel Movement Reporting System (VMRS) area defined in Table 161.12(c) of § 161.12 of this chapter, and</p> <p>(B) Do not operate at speeds in excess of 14 knots; and</p> <p>(iii) Vessels identified in paragraph (b)(1)(iv) of this section engaged in dredging operations.</p> <p>(c) <i>SOLAS provisions</i>. The following self-propelled vessels must comply with</p>		
--	---	--	--

	<p>International Convention for Safety of Life at Sea (SOLAS), as amended, Chapter V, regulation 19.2.1.6 (Positioning System), 19.2.4 (AIS Class A), and 19.2.3.5 (Transmitting Heading Device) or 19.2.5.1 (Gyro Compass) as applicable (Incorporated by reference, see § 164.03):</p> <p>(1) A vessel of 300 gross tonnage or more, on an international voyage.</p> <p>(2) A vessel of 150 gross tonnage or more, when carrying more than 12 passengers on an international voyage.</p> <p>(d) <i>Operations</i>. The requirements in this paragraph are applicable to any vessel equipped with AIS.</p> <p>(1) Use of AIS does not relieve the vessel of the requirements to sound whistle signals or display lights or shapes in accordance with the International Regulations for Preventing Collisions at Sea, 1972 (72 COLREGS), 28 U.S.T. 3459, T.I.A.S. 8587, or Inland Navigation Rules, 33 CFR part 83; nor of the radio requirements of the Vessel Bridge-to-Bridge Radiotelephone Act, 33 U.S.C. 1201-1208, part 26 of this chapter, and 47 CFR part 80.</p> <p>(2) AIS must be maintained in effective operating condition, which includes--</p> <p>(i) The ability to reinitialize the AIS, which requires access to and knowledge of the AIS power source and password;</p> <p>(ii) The ability to access AIS information from the primary conning position of the vessel;</p> <p>(iii) The accurate broadcast of a properly assigned Maritime Mobile Service Identity (MMSI) number;</p> <p>(iv) The accurate input and upkeep of all AIS data fields and system updates; and</p> <p>(v) For those vessels denoted in paragraph (b) of this section, the continual operation of AIS and its associated devices (e.g., positioning system, gyro, converters, displays) at all times while the vessel is</p>		
--	--	--	--

<p>§ 164.46 Automatic Identification System</p>	<p>underway or at anchor, and, if moored, at least 15 minutes prior to getting underway; except when its operation would compromise the safety or security of the vessel or a security incident is imminent. The AIS should be re`ed to continuous operation as soon as the compromise has been mitigated or the security incident has passed. The time and reason for the silent period should be recorded in the ship's official log and reported to the nearest Captain of the Port or Vessel Traffic Center (VTC).</p> <p>(3) AIS safety-related text messaging must be conducted in English and solely to exchange or communicate pertinent navigation safety information (analogous to a SECURITE broadcast). Although not prohibited, AIS text messaging should not be relied upon as the primary means for broadcasting distress (MAYDAY) or urgent (PAN PAN) communications. (47 CFR 80.1109, Distress, urgency, and safety communications).</p> <p>(4) AIS application-specific messaging (ASMs) is permissible, but is limited to applications adopted by the International Maritime Organization (such as IMO SN.1/Circ.289) or those denoted in the International Association of Marine Aids to Navigation and Lighthouse Authorities' (IALA) ASM Collection for use in the United States or Canada, and to no more than one ASM per minute.</p> <p><i>Note to paragraph (d):</i> The Coast Guard has developed the "U.S. AIS Encoding Guide" to help ensure consistent and accurate data encoding (input) by AIS users. This Guide is available at our "AIS Frequently Asked Questions" (FAQ #2) World Wide Web page at https://www.navcen.uscg.gov. Although of great benefit, the interfacing or installation of other external devices or displays (e.g., transmitting heading device,</p>		
--	---	--	--

<p>§ 164.46 Automatic Identification System</p>	<p>gyro, rate of turn indicator, electronic charting systems, and radar), is not currently required except as denoted in § 164.46(c). Most application-specific messages require interfacing to an external system that is capable of their portrayal, such as equipment certified to meet Radio Technical Commission for Maritime Services (RTCM) electronic chart system (ECS) standard 10900 series.</p> <p>(e) <i>Watchkeeping.</i> AIS is primarily intended for use by the Master or person in charge of the vessel, or by the person designated by the Master or person in charge to pilot or direct the movement of the vessel, who must maintain a periodic watch for AIS information.</p> <p>(f) <i>Portable AIS.</i> The use of a portable AIS is permissible only to the extent that electromagnetic interference does not affect the proper function of existing navigation and communication equipment on board and such that only one AIS device may be transmitting on board a vessel at any one time.</p> <p>(g) <i>AIS Pilot Plug.</i> The AIS Pilot Plug on any vessel subject to pilotage by other than the vessel Master or crew must be readily available and easily accessible from the primary conning position of the vessel and permanently affixed (not an extension cord) and adjacent (within 3 feet) to a 120-volt 50/60 Hz AC power receptacle (NEMA 5-15).</p> <p>(h) <i>Exceptions.</i> The following vessels may seek up to a 5-year deviation from the AIS requirements of this section by requesting a deviation under § 164.55.</p> <p>(1) Vessels that operate solely within a very confined area (e.g., less than a 1 nautical-mile radius, shipyard, or barge fleeting facility);</p> <p>(2) Vessels that conduct only short voyages (less than 1 nautical mile) on a</p>		
--	---	--	--

	<p>fixed schedule (e.g., a bank-to-bank river ferry service or a tender vessel);</p> <p>(3) Vessels that are not likely to encounter other AIS-equipped vessels;</p> <p>(4) Vessels whose design or construction makes it impracticable to operate an AIS device (e.g., those that lack electrical power, have an exposed or open cabin, or are submersible); or</p> <p>(5) Vessels denoted in paragraph (b)(2) that seek a deviation from requirements in paragraphs (d)(2)(ii) and (e) of this section because their AIS Class B device lacks a display.</p> <p>(i) <i>Prohibition.</i> Except for maritime support stations (see 47 CFR 80.5) licensed by the Federal Communications Commission (FCC), broadcasts from AIS Class A or B devices on aircraft, non-self propelled vessels or from land are prohibited.</p> <p>(j) <i>Implementation date.</i> Those vessels identified in paragraphs (b) and (c) of this section that were not previously subject to AIS carriage must install AIS no later than March 1st, 2016 [eff. 81 FR 20250, 4/7/16].</p>		
<p>§ 164.46 Automatic Identification System (ADD-IN)</p>	<p><i>Note to paragraph (b):</i> Under 33 U.S.C. 1223(b)(3) and 33 CFR 160.111, a Coast Guard Captain of the Port (COTP) may restrict the operation of a vessel if he or she determines that by reason of weather, visibility, sea conditions, port congestion, other hazardous circumstances, or the condition of such vessel, the restriction is justified in the interest of safety. In certain circumstances, if a COTP is concerned that the operation of a vessel not subject to § 164.46 would be unsafe, the COTP may determine that voluntary installation of AIS by the operator would mitigate that concern.</p>	<p>SUFFICIENT: ESTABLISHES SPECIFIC INFORMATION REGARDING PREVIOUS SECTION, SPECIFICALLY ESTABLISHED CONDITIONS FOR VESSEL SAFETY AND VULNERABILITIES</p>	<p>ENFORCED: PROVIDES ENFORCEMENT BY SPECIFYING SOLELY WHAT COMPLIANCE FOR THE UNITED STATES LAW AS WELL AS ITS LAW FOR INTERNATIONAL LAW; CFR IS MORE STRINGENT ON ENFORCEMENT WITH AIS LAWS</p>

Source: Author own elaboration based on USCG CFR (2002)

The analysis of data presented on Table 4 and 5 show the various contrasts between international law and national law. The CFR/National laws tend to describe and explain AIS clearer and at more length than the IMO/International laws. Additionally, the results listed display, specifically for the AIS receptor, that there is potential that the system itself is a vulnerability. These laws, at a national and international level, distinctively are shown multiple differences as stated earlier, are not addressing the stringency of these laws.

Moreover, the international laws in Table A compared with the national laws are significantly broader; therefore, these laws are easily taken advantage over due to the numerous loopholes found in these international laws such as ways that countries under SOLAS can retrieve data for both its transmitters and receivers and also to check if the data is able to receive and transmit. The Code of Federal Regulations in Table B goes above and beyond in comparison to the IMO SOLAS Annex 12 and 17 laws in Table A because of their specifics with not only what is being addressed in each law but what also is being enforced. A quick observation of the two laws noted that the Table B laws are significantly lengthier than the Table A laws, which can result in the content of the laws and its specifics. Another consideration of the reason for the less amount of length in the international laws is most likely due to having a wider number of countries compliant to these laws, ranging from developed and developing nations.

However, the laws are missing separate legislation specifically for receptors. Both laws currently combine the receptors/receivers with the transponder/transmitter. This leaves specifics out for both the transmitters and receivers, resulting in loopholes for what actions can be passed and cannot be passed.

Still, vulnerabilities within AIS data include, per Lloyd's Register (2018), lack of "an inbuilt mechanism to encrypt or authenticate signals, considered a soft target for cyber attack."

Other vulnerabilities from Lloyd's Register (2018) include that "AIS communications do not employ authentication or integrity checks; communication is made over RF. Anyone with cheap RF receiver can also 'listen' to these messages. (Range dependent)." Attackers can easily compromise AIS which can prevent a ship from providing movement information due to spoofing, ghost-targeting, multipathing, and false reporting on emergencies. Online services are often misled due to these events. False signals can dominate the control of the receptors on a ship, causing ships to run off course and other dangerous situations. Additionally, Frantzman (2018) mentions "cloaking" is typically used as a way to hide a ship's movements by turning, or switching, off their AIS transponder or transmitter, resulting in a fiscal penalty if the culprit is found guilty and will be charged with a minimum of \$1,000 per each day the law was violated; however, these penalties are known to reach closer to \$5,000 to \$15,000. This action is seen from a range of vessels: from fishing boats to tankers. However, minimum information and research is mentioned regarding the AIS receptors.

CHAPTER V

CONCLUSION

Maritime cybersecurity is an area that should not go unnoticed. AIS, due to the initiation of IoT, represents a threat to the maritime cyber security. While the current literature focus on technical aspects, there is a current need of comparing the sufficiency and enforcement of existing laws associated with AIS transmission and reception. AIS within cyber security is underrated and undervalued, especially when compared to other known policies that have grown to be such a push and focus. Focusing within the United States, it is obvious to state that these vulnerabilities are an issue that should not be taken lightly within maritime time companies as it currently is.

This conclusion assesses the studies in regard to maritime cyber security with the use of AIS data, specifically in the United States. It provides areas within law that have not been addressed currently. Lastly, it will also identify the vulnerabilities within the areas lacking in law.

Focusing more on the national laws, the United States has significant increase in enforcement on the AIS laws in regard to AIS receiver equipment; however, there remains areas that have not been addressed in law and currently the USCG enforces civil penalties such as fines for every day a violation occurs. As these regulations for AIS data become more specific towards transponders and receptors, more awareness for these cyber crimes will be present as well as ways in which to mitigate.

Previous research shows that there have been discrepancies within the AIS data, which could be resolved having more laws specific to AIS data receptor equip maritime cybersecurity is an area that should not go unnoticed.

REFERENCE

- Biener, Christian, Eling, Martin and Wirfs, Jan Hendrik (2014) *Insurability of Cyber Risk: An Empirical Analysis*, The Geneva Papers, 2015, 40, (p. 131-158), 2015 The International Association for the Study of Insurance Economics 1018-5895/15. The Institute of Insurance Economics, University of St. Gallen, Switzerland.
- Cebula, J.J. and Young, L.R. (2010) *A Taxonomy of Operational Cyber Security Risks*, Technical Note CMU/ SEI-2010-TN-028, Software Engineering Institute, Carnegie Mellon University.
- CFR (2002). Automatic Identification System, United States Coast Guard Code of Federal Regulation, 33 § 164.46.
- Ferber, S., (2013). How the Internet of Things Changes Everything. *Harvard Business Review*: <https://hbr.org/2013/05/how-the-internet-of-things-cha/>
- Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. Lancaster University. Available at http://eprints.lancs.ac.uk/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf
- Frantzman, Seth J. (2018) "Avoiding Detection: The Team Tracking Iran's Attempt to Cloak Its Oil Exports." *The Jerusalem Post* | *JPost.com*, 25 Oct. 2018, www.jpost.com/Middle-East/Avoiding-detection-The-team-tracking-Irans-attempt-to-cloak-its-oil-exports-570236.
- HudsonAnalytix (2018). *Cybersecurity Risk Management: Understand, Manage & Respond*. CMA. CMA_March_2018_Cal_Maritime.pdf
- Hsia, Janelle. (2017). "Do You Know Your Risks?" American Cyber Security Management, 15 Dec. 2017, www.americancsm.com/do-you-know-your-risks/
- IALA (2016). *IALA Guideline 1082 – An Overview of AIS*. Edition 2.0. https://www.navcen.uscg.gov/pdf/IALA_Guideline_1082_An_Overview_of_AIS.pdf
- Kam, H. J., Ho, S. M., & Katerattanakul, P. (2016). Cyber Offense vs. Cyber Defense: A Theoretical Framework. Conference: JAIS Theory Development Workshop, December 2016, Dublin, Ireland.
- Kaspersky Lab (2013). "Java under Attack – the Evolution of Exploits in 2012-2013." Securelist English, securelist.com/kaspersky-lab-report-java-under-attack/57888/.
- Kusi, Bernard (2015). PORT SECURITY- Threats and Vulnerabilities. Laurea University of Applied Sciences.
- Lacy, P.; Keeble, J.; McNamara, R.; Rutqvist, J.; Haglund, T.; Cui, M.; Cooper, A.; Pettersson,

- C.; Kevin, E.; Buddemeier, P.; et al. Circular Advantage: Innovative Business Models and Technologies to Create Value in a World without Limits to Growth; Accenture: Chicago, IL, USA, 2014
- Lloyd's Register (2018). *LR approach to cyber security – Marine and Offshore* LLOYD'S REGISTER.
<https://www.rina.org.uk/res/LR%20Approach%20to%20Cyber%20Security.pdf>
- Merriam-Webster (2011). Springfield, MA: Merriam-Webster Incorporated.
- Mileski, J.P., Clott, C., Galvao, C.B. (2017). Cyberattacks On Ships: A Wicked Problem Approach. Proceeding of the International Association of Maritime Economists Annual Conference, 2017, Kyoto, Japan.
- Mileski, J.P., Clott, C., Galvao, C.B. Cyberattacks On Ships: A Wicked Problem Approach. Maritime Business Review 3, no. 4 (2018): 414-430. <https://doi.org/10.1108/MABR-08-2018-0026>
- Mukhopadhyay, Arunabha & Saha, Debashis & Mahanti, Anirban & B B, Chakrabarti & A, Podder. (2005). Insurance for Cyber-risk: A Utility Model. Decision. 32.
- National Institute of Standards and Technology (NIST) (2018), *Components of The Cybersecurity Framework*. National Institute of Standards and Technology: U.S. Department of Commerce.
- RayMarine. "Automatic Identification System (AIS)." RayMarine.com, 2017, www.raymarine.com/uploadedFiles/Blog/Raymarine_Blog/AutomaticIdentificationSystem.pdf.
- Robinson, Adam (2015). 4 Uses of Supply Chain Technology Applications Moving Shippers into the Future of Effective Management: Infographics Logistics Supply Chain Technology; Available at <http://cerasis.com/2015/10/14/supply-chain-technology-applications/>
- Salem, Walid (2018). Best Practices for Finding Cyber Threats and Vulnerabilities. The Maritime Executive.
- SOLAS (2015). Automatic Identification System, International Maritime Organization, 33 SOLAS Annex 12 & 17. (<http://solasv.mcga.gov.uk/Annexes/Annex17.htm>)
- Wang, P. and Mileski, J.P. (2018). A Contingency and Network Framework in Integrating Maritime Transportation Decisions through Global Supply Chains. Proceeding of the International Association of Maritime Economists Annual Conference, 2018, Mombasa, Kenya.